PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-232960
(43)Date of publication of application : 14.09.1990

(51)Int.Cl. H01L 27/04
H01L 21/82
H01L 29/788
H01L 29/792

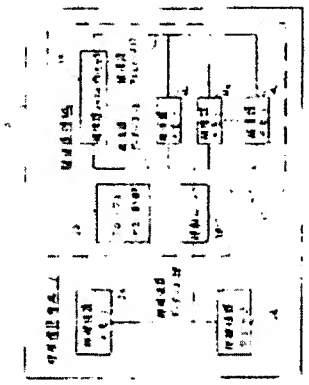
(21)Application number : 02-004397
(22)Date of filing : 11.01.1990

(71)Applicant : GENERAL INSTR CORP
(72)Inventor : GILBERG ROBERT C
KNOWLES RICHARD M
MORONEY PAUL
SHUMATE WILLIAM A

(30)Priority
Priority number : 89 297472 Priority date : 12.01.1989 Priority country : US

(54) INTEGRATED CIRCUIT CHIP

(57)Abstract:
PURPOSE: To ensure an integrated circuit chip of data protection by a method wherein a semiconductor layer is partitioned into a protected region and a non-protected region, a microprocessor and a memory to protect are provided in the protected region, and a memory and a logic which control them are provided in the non-protected region, and the two partitioned regions are connected with a conductive layer.
CONSTITUTION: An IC chip 10 is partitioned into a protected region 11 and a non-protected region 12, wherein a microprocessor 14 which processes the protected data, memories M1 to M4 which store the protected data, a data bus 16, an address bus 17, a transfer logic circuit 18, and a circuit 20 which controls clock and a power are provided in the protected region 11. A non- protected memory 24 and a non-protected logic 26 are provided in the non- protected region 12, and the outputs of them are inputted into the logic 18 located in the region 11 through the intermediary of the data bus 28. Thereafter, signals selected by the logic 18 are inputted



15

into the prescribed device located in the region 11, whereby the protected data are prevented from being erroneously inspected and modified.

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2-232960

⑤Int. Cl.[5]	識別記号	庁内整理番号			⑬公開 平成2年(1990)9月14日
H 01 L 27/04	A	7514-5F			
		7514-5F	H 01 L	29/78	3 7 1
		8526-5F		21/82	D※

審査請求 未請求 請求項の数 24 (全13頁)

⑤④発明の名称　集積回路チップ

⑳特　願 平2-4397
㉒出　願 平2(1990)1月11日
優先権主張 ㉜1989年1月12日㉝米国(US)㉛297,472

⑦②発明者　ロバート・シー・ギルバーグ　アメリカ合衆国、カリフオルニア州 92131、サンデイエゴ、カミニート・ガルシア 11484
⑦②発明者　リチヤード・エム・ノウルズ　アメリカ合衆国、カリフオルニア州 92126、サンデイエゴ、ヘンプヒルウエイ 10323
⑦①出願人　ジエネラル・インストルメント・コーポレーション　アメリカ合衆国、ニユーヨーク州、10153 ニユーヨーク、フイフス・アベニユー 767
⑦④代理人　弁理士 鈴江 武彦　外3名
最終頁に続く

明　細　書

1. 発明の名称

集積回路チップ

2. 特許請求の範囲

(1) 被保護データが処理並びに／又はストアされる被保護領域(11)を有する集積回路チップ(10)であり、

回路要素部品を形成する拡散部分(S, D)を有する半導体層(SC)と、

被保護データを配分、ストア、処理並びに／又は変更をするための回路要素(14,16,17,18,20,M_1, M_2, M_N)を形成する要素相互を接続するように前記半導体層と結合される第一導電層(CN_1)と、

前記回路要素が検査からシールドされた被保護領域(11)を形成するように回路要素を覆うと共に、回路要素の予期機能に対し、必須の所定の信号を回路要素に送り込むために回路要素と接続された第2導電層(CN_2)とを具備し、前記第2導電層の除去は、所定の必須の信号が回路要素へ送られることを妨げ、予期機能をはばむ集積回路チップ。

(2) 前記所定の信号がパワー信号である請求項(1)に記載の集積回路チップ。

(3) 前記シールドされた回路要素が被保護データをストアするための揮発性メモリ(M_1, M_2, M_N)を有し、このメモリは所定のパワー信号で動かされる請求項(2)に記載の集積回路チップ。

(4) 前記揮発性メモリ(M_1, M_2, M_N)が夫々個別に、夫々のメモリと第2導電層(CN_2)の重った場所のみから所定のパワー信号を受けられるように第2導電層のその場所のみと接続されたメモリである請求項(3)に記載の集積回路チップ。

(5) 非被保護データと制御信号が処理並びに／又はストアされ、前記のシールドされた回路要素は被保護領域(11)と非被保護領域(12)間の非被保護データ並びに／又は制御信号のトランスファーを可能にする所定のパワー信号で動作するロジック回路要素(18)を含むような非被保護領域(12)を

さらに具備した請求項(2)に記載した集積回路チップ。

(6)前記のロジック回路要素(18)が夫々個別に第2導電層の重なった場所からのみ所定のパワー信号を受けるようにロジック回路要素と重った第2導電層（CN_2）のその場所に別々に接続されている請求項(5)に記載した集積回路チップ。

(7)前記のシールドされた回路要素(14,16,17,18,20,M_1, M_2, M_N)が夫々個別に第2導電層の重った場所のみからのみ所定のパワー信号を受けるようにシールドされた回路要素と重った第2導電層（CN_2）のその場所に別々に接続されている請求項(2)に記載した集積回路チップ。

(8)前記の第1導電層のシールドされた回路要素は被保護データをストアするためのメモリ（M_1, M_2, M_0）と、そのメモリにストアされる駆動データ用のロジック回路(14)を有し，その第2導電層（CN_2）はロジック回路の駆動機能にとって必須である信号を導き、そしてこの第2導電層の除去はこのメモリにデータがストアされることを妨げるような請求項(1)に記載の集積回路チップ。

(9)前記のシールドされた回路要素が変更不能な被保護データをストアするための所定の夫々場所としてメモリロケーションをもったメモリ（M）と、

アドレスバスに伝えられたアドレス信号により指示されたメモリの場所にデータがストアされるためにこのメモリとアドレスバス(46)に接続されたメモリ制御ロジック回路(38)と、

最初の状態と非可逆的に変化した状態を持つフューズ要素(42)と、

所定の制御信号(48)に呼応してフューズ要素の状態を非可逆的に変化させるためのフューズ要素に接続されたもの(44)と、

フューズ要素の状態と所謂アドレス信号をモニターするためと、何時でも所定のメモリロケーションがアドレスバス上でアドレス信号により示されるが、ヒューズ要素が非可逆的に変化してしまったあとではメモリ制御回路がデータを所定のメモリロケーションにストアさせるのを妨げるためにフューズ要素とメモリ制御回路とアドレスバスとに接続されたデテクター(40)と

を備えた請求項(1)に記載された集積回路チップ。

(10)前記第2導電層（CN_2）が更にメモリ（M）と、メモリ制御ロジック回路(38)と、デテクター(40)と、フューズ要素(42)とを直接的外部からのアクセスからシールドしている請求項(9)に記載された集積回路チップ。

(11)前記所定の信号が、メモリ（M）と、メモリ制御ロジック回路(38)と、デテクター(40)とが所定のパワー信号で動作されるようなパワー信号である請求項(9)に記載された集積回路チップ。

(12)前記所定の信号がパワー信号であり、メモリ（M）は所定のパワー信号で動作する揮発性メモリである請求項(9)に記載された集積回路チップ。

(13)前記シールドされた回路要素が、

変更不能な被保護データをストアするための所定のメモリロケーションを持っている第1メモリ（M）と、

第2メモリ(52)と、

第2メモリにデータパターンをストアさせる手段(55)と、

第2メモリが所定のデータパターンを持っている時は何時でも書込み信号(64)に呼応して第1メモリの所定のロケーションにデータをストアさせられるように第1と第2メモリに接続されたメモリ制御ロジック回路(55)と、

第2メモリの内容を消去出来るように第2メモリに接続された手段(66)と、

最初の状態と非可逆的に変化した状態をもつヒューズ要素(50)と、

所定の制御信号(67)に呼応してフューズ要素を非可逆的に変化させるフューズ要素に接続されている手段(58)と、

フューズ要素の状態が非可逆的に変化する前にのみ所謂データパターンがストア出来るようにするデータパターンを第2メモリにストアするもの

に接続されたフェーズ要素とを備えた請求項(1)に記載された集積回路チップ。

(14)前記第２導電層（CN_2）が更にメモリ（M,52)と、メモリ制御ロジック回路(54)と、ストレッヂ用部品とフューズ要素とを直接的外部からのアクセスからシールドしている請求項(13)に記載の集積回路チップ。

(15)前述の所定の信号がパワー信号であり、メモリ（M,52)とメモリ制御ロジック回路(54)と、ストレッヂをさせる部品とが所定のパワー信号で動く請求項(13)に記載の集積回路チップ。

(16)前述の所定の信号がパワー信号であり、第１メモリ（M）が所定のパワー信号で動作する揮発性メモリである請求項(13)に記載の集積回路チップ。

(17)シールドされた回路要素が、

被保護データをストア出来る動作部品(60)と、

最初の状態と非可逆的に変化した状態をもつフューズ要素(58)と、

所定の制御信号に呼応してフューズ要素の状態を非可逆的に変化させる、フューズ要素に接続された手段(58)とを備え、

そのフューズ要素がその状態が非可逆的変化をする前にのみ所謂被保護データをストア出来るようにする手段と接続されているような請求項(1)に記載の集積回路チップ。

(18)前記の所定の信号が、パワー信号であり、動作部品(60)は所定のパワー信号で動作する請求項(17)に記載の集積回路チップ。

(19)所謂テスト回路要素に対するアクセス回路要素に対する部品(78)と、

最初の状態と非可逆的に変化した状態をもつフューズ要素(70)と、

所定の制御信号(80)に呼応してフューズ要素の状態を変化させる、フューズ要素に接続された部品(74)とを備え、

そのフューズ要素が、その状態が非可逆的に変化する前にのみ所謂テストのためにアクセス出来る手段に接続されているような請求項(1)に記載の集積回路チップ。

(20)前記所定の信号はパワー信号であり、作動部品(72,74)は第２導電層により外部よりのアクセスからシールドされ、所定のパワー信号で動作する請求項(19)に記載の集積回路チップ。

(21)前記のシールドされた回路要素に、

被保護データをストアし、処理し、処理に影響を与える前述の回路要素（M）と、

最初の状態と非可逆的に変化した状態をもつフューズ要素(42)と、

所定の制御信号(48)に呼応してフューズ要素の状態を非可逆的に変化させる、フューズ要素に接続された部品(44)と、

フューズ要素(42)と前記回路要素（M）に接続され、

フューズ要素の状態をモニターするためと、フューズ要素の状態が非可逆的に変化してしまったあとで回路要素の予期状態を妨げるための手段(40)が含まれる請求項(1)に記載された集積回路チップ。

(22)シールドされた回路要素には、

被保護データをストアし、処理し、処理に影響を与える前述の回路要素（M）と、

最初の状態と非可逆的に変化した状態をもつフューズ要素(42,58)と、

フューズ要素に接続され、所定の制御信号(48,87)に呼応してフューズ要素の状態を変化させる部品(44,58)を有し、

このフューズ要素は、その状態が非可逆的に変化する前にのみその回路要素の予期機能が可能となるように回路要素と接続されている請求項(1)に記載した集積回路チップ。

(23)シールドされた回路要素に更に被保護データをストア並びに／又は処理するシールドされた回路要素(14,M_1, M_2, M_n)への供給パワーを制御する手段(20)を有する請求項(1)に記載の集積回路チップ。

(24)シールドされた回路要素に更にクロック信号を発生させそのクロック信号を被保護データをストア並びに／又は処理するシールドされた回路要素(14,M_1, M_2, M_n)に供給する手段(20)

を有する請求項(1)もしくは(23)に記載された集積回路チップ。

3．発明の詳細な説明

［従来の技術］

本発明は一般に電子的データ処理システム用集積回路チップに関し、特に集積回路チップの被保護領域でストアされたり処理された被保護データの検査や修正を防止することを指図する。

被保護データを処理しストアする集積回路チップは被保護データを処理しストアする回路要素をもった被保護領域と、非保護データと制御信号を処理しストアする回路要素をもつ非被保護領域とを備えている集積回路チップは回路要素を形成する拡散部を有する半導体層と、回路要素を形成する部品を内部接続するために前記半導体層と接続された第1導電層を具備する。すべての新しい集積回路チップは代表的には回路要素と部品を相互接続するために1つ或はそれ以上の導電層を有する。一般的にこれ等の層は制御信号とパワー信号両者を伝えるのに使われ、信号の相互接続の密度を最大とし、そのような相互接続に要な面積を減少させることを目標としている。

この被保護領域は更に、被保護領域内にあるデータ処理回路要素により被保護データを処理するために被保護領域内のデータバスへ非被保護データと制御信号を転送する回路要素を有する、被保護領域内の回路要素は非被保護データと制御信号を非被保護領域と被保護領域内のデータバス間に被保護領域内のデータ処理回路要素により発生された制御信号に応じて転送することができる。

［発明が解決しょうとする課題］

それにも拘わらず、被保護データでさえこのような集積回路チップでは被保護領域から非被保護領域への転送は容易には出来ず、被保護領域内にストアされたか、処理中の被保護データに例えば走査形電子顕微鏡（ＳＥＭ）やここから被保護データがアクセス出来る被保護領域内で与えられたノードで顕微鏡に接続されたプローブのような診断装置を使った検査によりアクセスをすることができる。又特定の制御信号を被領域内のロジック回路要素に送ることによりプローブのような方法でロジック回路が被保護データを被保護領域内の非被保護と被保護再データを被保護領域内のデータ処理回路要素により処理するため、データバスから非被保護領域へ転送することが出来るかもしれない。或は被保護領域内のストアされた被保護データはチップの保護を疑わしくされることを意味することが出来内密のデータによりおきかえられるかもしれない。

［課題を解決するための手段］

この発明は、回路要素部品を形成する拡散部分を有する半導体層と、

被保護データを配分、ストア、処理並びに／又は変更をするための回路要素を形成する要素相互を接続するように前記半導体層と結合される第一導電層と、前記中で、回路要素が検査からシールドされた被保護領域を形成するように回路要素を覆うと共に、回路要素の予期機能に対し、必須の所定の信号を回路要素に送り込むために回路要素と接続された第2導電層とを具備し、前記第2導電層の除去は、所定の必須の信号が回路要素へ送られることを妨げ、予期機能をはばむ、被保護データが処理並びに／又はストアされる被保護領域を有する集積回路チップを提供する。

この発明の一態様においては、前記所定の信号がパワー信号である。この一態様に係わる実施例においては、前記第1の導電層のシールドされた回路要素が被保護データをストアするための揮発性ランダムアクセスメモリ（ＲＡＭ）を有し、このメモリは所定のパワー信号で動かされ、この結果、メモリの検査を可能にする第2の導電層の除去はパワーがメモリーから除去される。メモリが揮発性のために、これからパワーを除去するのはメモリにストアされている被保護データを消去することになる。

前記一実施例において、前記複数の揮発性メモリが夫々個別に、夫々のメモリと第2導電層の重った場所のみから所定のパワー信号を受けられるように第2導電層のその場所のみと接続され、この結果、メモリを検査するためためにメモリを覆

っている第２の導電層の部分のみの除去は、この除去により露出したメモリからパワーが除去されるので、不都合である。

この発明に係わる集積回路チップにおいては、さらに非被保護データと制御信号が処理並びに／又はストアされ、前記のシールドされた回路要素は被保護領域と非被保護領域間の非被保護データ並びに／又は制御信号のトランスファーを可能にする第２の導電層により与えられる所定のパワー信号で動作するロジック回路要素を含むような非被保護領域をさらに具備する。この結果、被保護データがチップの非被保護領域に被保護領域から伝達されるのを可能にするプローブのような手段により、制御信号がロジック回路要素に送られるのを可能にするための第２の導電層の除去は、このような第２の導電層の除去がまたロジック回路要素からパワーを除去するので、好ましくない。このような実施例において、前記のロジック回路要素が夫々個別に第２導電層の重なった場所からのみ所定のパワー信号を受けるようにロジック回路要素と重った第２導電層のその場所に別々に接続されている。

この発明の別の態様において、前記の第１導電層のシールドされた回路要素は被保護データをストアするためのメモリと、そのメモリにストアされる駆動データ用のロジック回路を有し，その第２導電層はロジック回路の駆動機能にとって必須である信号を導き、しかもこの第２導電層の除去はこのメモリにデータがストアされることを妨げる。この結果、秘密データがチップの意図とした保護を損なう被保護データにメモリで代わられるのを可能とするロジック回路に制御信号を送るための第２の導電層の除去は、この第２の導電層の除去がロジック回路によってメモリにストフされるデータとなることを妨げるので好ましくない。

［実施例］

第１図に於て、本発明の集積回路チップ１０の好ましい実施例は被保護領域１１と非被保護領域１２とを備えている。チップ１０はＶＬＳＩ(Very Large Scale Integrated) 回路チップである。このチップ１０は被保護領域１１内に次の回路要素を形成している。即ち、被保護データを処理するマイクロプロセッサー１４と、被保護データをストアする複数のメモリM_1，N_2，M_nと、被保護データバス１６と、被保護アドレスバス１７と、移転ロジック回路１８と、被保護クロック並びにパワー制御回路２０とである。このチップ１０はこのような回路要素の特別な混ぜ合せである必要はなく、その中で被保護データが無承諾の読み取り或は被保護データ並びに／又は指令の変更に対し保護されているような回路要素の或る組合せであってもよい。このメモリM_1，M_2，M_nはどんなタイプでもよく、例えばＲＡＭ（ランダムアクセスメモリ）、ＲＯＭ（読みとり専用メモリ）、ＥＰＲＯＭ（電気的書込可能な読み取り専用メモリ）、ＥＥＰＲＯＭ（電気的消去書込可能な読み取り専用メモリ）等や、レジスタファイルやＦＩＦＯ（ファストイン／ファストアウト）バッファ等である。

導電層CN_2は回路要素１４，M_1，M_2，M_n，１６，１７，１８，２０を検査からシールドするためにこれらを覆っておりこうして被保護領域１１を形成している。

非被保護領域１２の中で、チップ１０は次の如き回路要素を形成している。即ち、メモリ２４とロジック回路２６と非被保護データバス２８とを形成している。

ＭＯＳ回路要素を含むチップ１０の実施例では第２図と第３図とに示す如く、このチップは半導体基板層ＳＣと第１絶縁層DE_1と、第１導電層CN_1と、第２絶縁層DE_2と、第２導電層CN_2と、第n番目の絶縁層DE_Nと、n番目の導電層CN_nとを有する。半導体基板層ＳＣの中の拡散部分ＳとＤは、ソースとドレンを形成し、それ等はゲート導体Ｇと組合され第１導電層CN_1により相互で接続されることでチップ１０の回路要素を形成するために勢揃いしている相補性ＭＯＳ電界効果トランジスタを形成している。第１導電層CN_1は第１絶縁層DE_1の孔を通し、導体３０によりソースＳとドレンＤと接続されて

いる。第２導電層ＣＮ$_2$は第２絶縁層ＤＥ$_2$にある孔を通し、導体３１により、シールドされた回路要素の予期機能に必須である所定の信号を回路要素に伝えるため第１導電層と接続されている。

第２導電層ＣＮ$_2$を除去することはこの回路要素に所定の必須の信号を伝えることを妨げ、従って予期機能もはばむことになるであろう。第２導電層ＣＮ$_2$は回路要素を覆い、その中で回路要素が検査からシールドされた被保護領域１１を形成している。

バイポーラ回路要素を有するチップ１０の実施例では、第４図に示す如く、このチップは半導体基板層ＳＣと、第１絶縁層ＤＥ$_1$と、第１導電層ＣＮ$_1$と、第２絶縁層ＤＥ$_2$と、第２導電層ＣＮ$_2$と、第ｎ番目の絶縁層ＤＥ$_n$と、ｎ番目の導電層ＣＮ$_1$とを有している。半導体層ＳＣ内の拡散部ＣとＢとＥは、コレクタと、ベースと、エミッタとを形成し、これらはチップ１０の回路要素を形成勢揃いしているバイポーラトランジスタを形成するために第１導電層ＣＮ$_1$により相互接続されている。第１導電層ＣＮ$_1$は第１絶縁層ＤＥ$_1$にある孔を通し、導体３２によりシールドされた回路要素の予期機能に必須である所定の信号を回路要素に伝えるためコレクタＣと、ベースとに接続されている。第２導電層ＣＮ$_2$は第２絶縁層ＤＥ$_2$にある孔を通じ導体３３によりシールドされた回路要素の予期機能に必須である所定の信号を回路要素に伝えるため第１導電層ＣＮ$_1$と接続されている。

第２導電層ＣＮ$_2$の除去は、この回路要素に所定の必須の信号を伝えることを妨げ従って予期機能もはばむことになるであろう。第２導電層ＣＮ$_2$は回路要素を覆い、その中で回路要素が検査からシールドされた被保護領域１１を形成している。

被保護データを配分し、ストアし処理し或は影響を与えるチップ１０のすべての回路要素は、相互接続層ＣＮ$_1$の如き、あらかじめ作り込まれ、層ＣＮ$_2$の如く、シールドの特性を持ち、被保護領域１１の境界を形成している導電層の下に位置する導電層を利用している。

第２導電層ＣＮ$_2$は機械的とＳＥＭ（走査型電子顕微鏡）のプロビングに対するシールドとしての機能と、その下にある回路要素を動作不能にすることなしに除去出来ぬ所定の必須信号を伝達する層としての機能とを有する。所定の必須信号はパワー信号でも命令の如き制御信号でもよい。所定の必須信号がパワー信号である場合検査の目的でのシールド層ＣＮ$_2$の除去は機械的であれ化学的であれ或はその他の手段であれ下にある回路要素からパワーを除くこととなり動作不能にし更に多分同じ回路要素にストアされている何かのデータやロジックステートを失わせることになるだろう。

この技術は、特に揮発性ＲＡＭの如き揮発性メモリにストアされている被保護データを守るのに有効である。その中のメモリＭ$_1$とＭ$_2$とが揮発性メモリであるチップ１０の実施例に於て、このメモリＭ$_1$とＭ$_2$は夫々検査からシールドするため第２導電層ＣＮ$_2$により覆われている。そして、パワー信号は別々に夫々のメモリＭ$_1$，Ｍ$_2$と重っている第２導電層ＣＮ$_2$のポーションから夫々のメモリＭ$_1$，Ｍ$_2$に分配される。この分配は第５図に示され、第２導電層ＣＮ$_2$は揮発性メモリの中のトランジスタのソースＳに導体３４によりメモリパワーを配分するため接続されている。夫々のメモリＭ$_1$，Ｍ$_2$を検査するため第２導電層ＣＮ$_2$の重ったポーションを除去することは、夫々のメモリＭ$_1$，Ｍ$_2$からパワーを除くこととなる。メモリＭ$_1$，Ｍ$_2$は揮発性であるからそこからパワーを除くことはその中にストアされた被保護データを削除することとなる。従ってメモリＭ$_1$，Ｍ$_2$の内容をそのメモリに重っている第２導電層ＣＮ$_2$のポーションのみを除くことで検査しようと試みても無駄であろう。

第６図に示した他の実施例に於て、パワー信号Ｖccは第２導電層ＣＮ$_2$から複数の揮発性メモリ要素Ｍに前述の実施例よりも少ない大きさですむ方法、その中ではパワーは夫々のメモリ要素と重った第２導電層のポーションのみからメモリ要素

に別々に配分されるような方法で配られる。この実施例では夫々のメモリ要素Mの列は下にある別々の第1導電層CN_1を経由して重った第2導電層CN_2からパワーを受けとる。この第2導電層CN_2は夫々の第1導電層CN_1に導体35により接続されている。この実施例が面積効率を上げるため多少の安全を失ってもこれ等のメモリ要素Mを、第2導電層CN_2の除去によるパワー損失によるデータの消去を起すことなしに検査しようとすることはすべての中間層接続導体35とそれにパワーを供給する第2導電層CN_2のポーションに触れずにすると同時に非常に高い分解精度のある第2導電層の除去が求められるであろう。

今一度第1図に於て、非被保護領域12の中ではロジック要素26とメモリ24とは非保護データと制御信号を処理しストアする。非保護データと制御信号は非被保護データバス28から被保護領域11にある被保護データバス16に移転ロジック回路18により転送される。移転ロジック回路18は非被保護データと制御信号を被保護領域11にある被保護データバス16にマイクロプロセッサ14により被保護データと処理するために転送する。転送ロジック回路18は非被保護データが被保護データバス16にある時に示すマイクロプロセッサ14により起される制御信号に呼応して非被保護データと制御信号が非保護データバス28と被保護データバス16の間に移転出来るようにする。マイクロプロセッサ14は被保護データバス16にあるデータ信号をモニターしロジック回路18が、データ信号と制御信号を非被保護データバス28と被保護データバス16の間に、非被保護データが被保護データバス16上にある間のみ転送可能とする制御信号を発生する。

上述の如く、導電層CN_2は移転ロジック回路18を検査からシールドする為に移転ロジック回路18に重っている。この導電層CN_2は又パワー信号を移転ロジック回路18に伝える。従って、移転ロジック回路18を検査する目的で導電層CN_2を除去することは移転ロジック回路18からパワーを除くことになり移転ロジック回路18が何かのデータ或は制御信号を被保護データバス16と非被保護データバス28の間に移転することを妨げる。

この技術は逆方向にも拡張出来る。従って秘密のデータは非被保護領域12から被保護メモリM_1, M_2, M_nに書き込まれることはない。マイクロプロセッサ14は被保護データバス16にあるデータをメモリM_1, M_2, M_nにストア出来るようにするメモリアクセスロジック回路を備えており、シールドしている導電層CN_2はパワー信号をマイクロプロセッサ14に伝える。従って、制御信号をマイクロプロセッサ14のメモリアクセスロジック回路に伝えるため、従ってこのことはメモリM_1, M_2, M_nの中に内密のデータを被保護データの代りにすることが出来、従ってチップの予期された安全を危くすることとなるが、このためにシールドしている導電層CN_2を除去することは、この除去がマイクロプロセッサ14からパワーを除き従ってメモリアクセスロジック回路がメモリM_1, M_2, M_nにデータをストアさせることをさまたげるから無意味である。

1つの実施例に於ては被保護領域内のシールドされたロジック回路14，18は夫々別々にシールドしている導電層CN_2の重っているポーションのみからパワー信号を受けとるためにそのロジック回路14，18に重っているシールドしている導電層CN_2の夫々のポーションのみに接続されている。

第7図に示す実施例に於て、被保護信号はシールド層CN_2とCN_nの下にある導電層CN_1に配分される。そしてシールド信号（必須の制御或はパワー信号）は上に覆っているシールド層CN_2とCN_nに別々に配分される。1つのシールドしている導電層CN_nの境界は図中では実線で示され、他のシールドしている導電層CN_2の境界は図中に破線で示され、下にある導電層CN_1は図中ボカして示される。下にある導電層CN_1は完全に1つか或は他のシールドしている導電層CN_2とCN_nによりシールドされている。そして下にある導電層CN_1の1つのポーション

はシールドしている導電層CN_2とCN_nの両者によりシールドされている。

このシールド層CN_2とCN_nを化学的或は普通のレーザ或はマイクロプローブで導電層CN_1中の被保護信号にアクセスするために切断すると言う試みは導電層CN_1に於てシールド層CN_2とCN_nへ接続（短絡）されるか導電層CN_1とCN_2とCN_nで形成される回路でオープン回路が出来こととなる。従って、被保護信号と必須の信号の配分をばらばらにさせ導電層CN_1とCN_2とCN_nに接続されている回路要素の所期機能をチップ１０の所期機能を害するように変化させる。

チップ１０にストアされたある被保護データがそのチップの入った製品の製造中にその被保護データがストアされたあとは変更されないと云うことは極めて重要である。この目的を成就するため、チップ１０は所定のメモリロケーションにストアされた被保護データの変更を妨げるためのシステムを有している。このような予防システムの他の実施例を第８図と第９図とに示す。

第８図のシステムはメモリＭと、メモリ制御ロジック回路３８と、デテクタ４０と、フューズ要素４２と、フューズ変更素子４４を有する。このシステムはメモリＭに適用されその中に被保護データがストアされる夫々のメモリM_1，M_2，M_nがメモリＭとして含まれている。

このメモリＭはデータバス１６からの変更不能なデータをストアする所定のロケーションである複数のメモリロケーションを持っている。

メモリ制御ロジック回路３８はアドレスバス４６により"書込み"信号がライン４７上でメモリ制御ロジック回路３８から被保護メモリＭに与えられた場合ユーズデータがアドレスバス４６に与えられたアドレス信号により指示されたメモリＭのロケーションにストアされるためにメモリＭに接続されている。

フューズ要素４２は最初の状態と非可逆的に変化した状態を持っている。"フューズ要素"と云う言葉はフューズとアンチフューズを云っている。

フューズ要素はチップ１０の中で金属性導電層とポリシリコンの導電層の組合せで形成される。アンチフューズ要素はチップの中で金属性導電層或はポリシリコンの導電層或は両者の組合せで形成される。アンチフューズ要素はチップの半導体層の中は導体／酸化物導体構造或は導体／アモルファスシリコン／導体構造により形成されるP^+／N^+半導体接合のダイオードとP^-／N^-半導体接合のダイオードとにより作られる。

フューズ変更素子４４は被保護領域１１より外にあるターミナル５０からライン４８に来る所定の制御信号に呼応してフューズ要素４２の状態を非可逆的に変化させるためにフューズ要素４２と接続されている。更にライン４８の制御信号は被保護領域１１の内部にあるターミナル（図示していない）から供給される。

デテクター４０はフューズ要素４２の状態とアドレスバス４６のアドレス信号をモニターするためとメモリ制御回路３８が所定のメモリロケーションが、アドレス信号によりアドレスバス４６上に示される時は何時でもフューズ要素の状態が非可逆的に変更してしまったあとでメモリＭの所定のメモリロケーションにコージングデータがストアされるのを防ぐためにフューズ要素４２とメモリ制御回路３８とアドレスバス４６とに接続されている。

第２導電層CN_2は、メモリＭとメモリ制御ロジック回路３８とデテクター４０とフューズ要素４２とを外部からの直接アクセスからシールドしている。

メモリＭとメモリ制御ロジック回路３８とデテクター４０は第２導電層CN_2から来るパワー信号によって働かされるようにすべて第２導電層CN_2に接続されている。

第８図のシステムはメモリＭの所定のロケーションに最初からストアされた被保護データの変更を防ぐのに使われる。フューズ要素４２の状態が非可逆的に変化した場合、デテクター４０はアドレスバス４６のアドレス信号により示された所定のメモリロケーションに何らかの追加データが書

込まれるのを防ぐ。

第８図のシステム中のフューズ要素４２は又このチップを使っている製品がその使用者にとどく時に先だってのみ適用出来るある予備的な被保護データ処理機能、例えば被保護データの予備的処理或は被保護データを処理するインストラクションのローディングを行ったりそれに影響したりする他のシールドされた回路要素（図に示されていない）に接続されることもある。デテクター４０の如きものはフューズ要素をモニターするためと、フューズ要素の状態が非可逆的に変化したあとでは他のシールドされた回路要素の予期された機能を妨げるためにフューズ要素４２と他のシールドされた回路要素に接続されている。

多くのフューズ技術は、被保護集積回路チップの製造工程中工場でのみフューズすることを可能にする。例えば、ある工場は素子のよりよい長期信頼性を得るためにフューズが溶けたあと、ポリシリコン（或は他のフューズ材料）上に酸化物を成長させることを要求している。第９図にシステムは、別の製造者が工場でのフュージンクの後、被保護メモリＭへ被保護データを入力することを可能にしているが、被保護メモリＭの内容の変更を妨げている。

第９図のシステムはメモリＭと、ＥＰＲＯＭ或はＥＥＲＯＭ（電気的消去可能なＲＯＭ）の如き消去可能なメモリ５２と、メモリ制御ロジック回路５４と、エネーブリング回路（駆動回路）５５と、フューズ要素５６と、ＡＮＤゲート５７と、フューズ変更素子５８とを有する。メモリ制御ロジック回路５４はＡＮＤゲート６０と、ＡＮＤゲート６０と消去可能なメモリ５２とを結ぶインバータ６２、並びに配線を含むＮ接続とを備えている。インバータ６２はＡＮＤゲート６０への選ばれた入力とＡＮＤゲート６０を働かせるには必要な消去可能メモリ５２中に所定のデータパターンを形成する如き消去可能なメモリ５２中の選ばれたメモリロケーションとの間に接続されている。

メモリＭは変更不能な被保護データをストアする所定のロケーションである複数のメモリロケーションを持っている。

駆動回路５５は、書込駆動信号がライン６３を通じ駆動回路５５に加えられたとき、消去可能メモリ５２にデータパターンをストアされるようにする。

メモリ制御ロジック回路５４は消去可能なメモリ５２が所定のデータパターンを入れている時は何時でもライン６４からＡＮＤゲート６０への書込み信号に呼応して第１メモリＭの所定のロケーションにデータがストアされるようにメモリＭと消去可能なメモリ５２と接続されている。

消去可能なメモリ５２の内容はチップ１０の被保護領域１１の外部にある消去ターミナル６６から"消去"の制御信号が与えられることで消され得る。

フューズ要素５６は、最初の状態と非可逆的に変化した状態とを持っている。フューズ変更素子５８は被保護領域１１の外部にあるターミナル６８からライン６７に与えられる所定の制御信号に呼応してフューズ要素５６の状態を非可逆的に変化させるためにフューズ要素５６に接続されている。更にライン６７の制御信号は被保護領域１１の内部にあるターミナル（図示していない）から供給される。

データパターンはデータターミナル６９から供給されＡＮＤゲート５７を通じ消去可能なメモリに供給される。ＡＮＤゲート５７はフューズ要素５６が最初の状態にある間のみ消去可能メモリ５２にデータを書込ませることが出来るようにフューズ要素５６につながる１つの入力をもっている。

フューズ要素５６は又フューズ要素５６の状態が非可逆的に変化変化する前のみ消去可能なメモリ５２に所定のデータパターンをストアさせられるように駆動回路５５と接続されている。

消去可能なメモリ５２はＮビットが必要である。工場では、消去可能なメモリ５２とＡＮＤゲート６０とに接続されたインバータ６２に対応して所定の１，０のパターンがＡＮＤゲート６０がライン６４を通じメモリＭに"書込み"制御信号がパ

ス出来るように消去可能なメモリ５２に入れられる。１，０の所定のパターンが消去可能なメモリ５２に入れられたあと、フューズ要素５６の状態が非可逆的に変化されると所定のパターンは変更出来ない。この点で集積回路チップ１０の処理やパッケージングは接続可能となり消去可能なメモリ５２にストアされた所定のパターンを乱すことなく最終処理とパッケージングが出来るようになる。

チップ１０が別の製造者に出荷されたあと被保護データは被保護メモリＭにストアされる。それは消去可能なメモリ５２にストアされた所定のパターンは、インバータ６２によりメモリ制御ロジック回路５４に入れられた所定のパターンに匹適しているからである。

被保護データが被保護メモリＭにストアされると"消去"信号が消去可能なメモリ５２の内容を消去するために消去ターミナル６６に加えられても被保護メモリＭの中の被保護データは変化しない。第２導電層CN_2はメモリＭと、消去可能なメモリ５２と、メモリ制御ロジック回路５４と、駆動回路５５と、フューズ要素５６とを直接的外部からのアクセスからシールドしている。

この技術は第９図のシステムをチップ１０のカバー層を通し消去可能なメモリ５２を遠くからプログラム仕直せるような非常に正確なＸ線ビームのショットや他の複雑な手段から守ることが出来る。この技術の安全はＥＥＲＯＭやＦＰＲＯＭの内容を遠くからプログラムし直すこと或はとけたフューズを再接続することは非常に困難だと云うことに由っている。若し非常に強力な焦点の定まらない或は発散性Ｘ線或は他の手段が、ＥＥＲＯＭ或はＥＰＲＯＭの内容を本質的に無作為化することが出来るとすれば、攻撃者は駆動パターンを完成させる企をくりかえすこととなる。従って安全はＥＥＲＯＭ或はＥＰＲＯＭセルがこれ等の状態によって偏よって設けられる。

第９図に示すシステムのフューズ要素５６は、所定の前被保護データプロセス機能を果たすように、他のシールド回路要素（図示せず）に接続され得る。この機能は、被保護データの前処理や被保護データの処理のための検査のように、チップを含む製品が製品の使用者に渡る前にのみ適用できる。フューズ要素５６は、フューズ要素５６の状態が非可逆的に変更される前にのみ、他のシールド回路要素の意図した機能が果たせるように、他のシールド回路要素に接続される。

第８図並びに第９図に示す被保護データ変更防止システムは"Prevention of Alternation of Data Stored in Secure Integrated Circuit Chip Memory"と題する同じ出願人による先願の主題である。

複雑な集積回路の製造は、全ての回路素子が正確に動作するようにするテスト操作の間、内部回路素子への完全なアクセスを必要とする。しかし、テストのための高いアクセス可能性は、被保護データもしくは変更されないデータを含むチップに対しては問題である。

第１０図は、テスト動作が完了した後に、テスト信号パスを永久的に無能にし、この結果チップの外部ピンからの内部被保護データ回路要素へアクセスをさらにする必要を無くすシステムを示す。このシステムはフューズ要素７０と、第１並びに第２のインバータ７２，７４と、抵抗７５と、第１並びに第２のＮＡＮＤゲート７６，７８と、フューズ変更装置７９とを有する。

前記フューズ要素７０は最初の状態と、非可逆てきに変化した状態とを呈する。フューズ変更装置７９はフューズ要素７０に接続され、被保護領域１１の外部のターミナル８１からライン８０により受信する所定の制御信号に応答して、フューズ要素７０の状態を非可逆的に変化させる。代わって、ライン８０への制御信号は被保護領域１１の内部のターミナル（図示せず）から受信する。

前記フューズ要素７０とインバータ７２，７４とは第１のＮＡＮＤゲート７６への１つの入力に直列に接続されている。このＮＡＮＤゲート７６の出力信号は外部テストデータ出力ターミナルに与えられる。

前記フューズ要素７０とインバータ７２，７４とは、また第２のＮＡＮＤゲートの出力ターミナル８２の１つの入力に直列に接続されている。

前記第２のＮＡＮＤゲート７８は、チップ１０の被保護領域１１内のテストコマンド入力ノード８６への外部テストコマンド入力ターミナル８４からのテストコマンド信号を通す。テストコマンド入力信号がテストコマンド入力ノード８６に与えられるのに応答して、テストデータがチップ１０の被保護領域１１内のテストコマンド出力ノード８８に与えられる。内部テストデータ出力ターミナルに与えられるテストデータは、回路要素１４，M_1，M_2，M_n，１６，１７，１８，２０（第１図に示す）のようなチップ１０の被保護データ要素からアクセスされ得る。

前記テストデータは、フューズ要素７０が最初の状態のときにのみ、テストコマンド出力ノード８８から、第１のＮＡＮＤゲート７６を介して、外部テストデータ出力ターミナル８２に与えられる。

また、テストコマンド入力信号は、フューズ要素が最初の状態の時にのみ、外部テストコマンド入力ターミナル８４から内部テストコマンド入力ノード８６に与えられる。

前記第２の導電層CN_2は、直接的な外部アクセスから、フューズ要素７０と、インバータ７２，７４と、抵抗７５と、ＮＡＮＤゲート７６，７８とをシールドする。

前記インバータ７２，７４と、抵抗７５と、ＮＡＮＤゲート７６，７８とは、全て第２の導電層CN_2に接続され、第２の導電層CN_2からのパワー信号により駆動される。

プローブによる被害を防止するように、可能な限りチップ１０内に深く、フユーズ要素７０から第１並びに第２のＮＡＮＤゲート７６，７８への信号パスを埋め込むことにより、付加的保護がなされる。かくして、フユーズ要素７０から第１並びに第２のＮＡＮＤゲート７６，７８への信号パスは、主として、N^+，P^+拡散により形成される。同様に最小の保護で、ポリシリコン並びに他の導電層が使用され得る。最上の導電層CN_n，CN_{n-1}の使用は避けることが好ましい。

４．図面の簡単な説明

第１図は本発明による集積回路チップのブロックダイヤグラムである。

第２図は本発明による集積回路チップにおけるＭＯＳ回路要素を示す断面図である。

第３図は回路要素をシールドしシールドされたＭＯＳ回路要素へ所定の信号を送る重った導電層を示す平面図である。

第４図は本発明の集積回路チップにおけるバイポーラ回路要素のシールデングを示す断面図である。

第５図は回路要素をシールドしシールドされた回路要素に電力を供給するための重った導電層を示す断面図である。

第６図は複数の揮発性メモリをシールドしている別の実施例のブロックダイヤグラムである。

第７図は回路要素の機能へ必須信号を送る重った導電層を示す平面図である。

第８図は被保護領域内で所定のロケーションにストアされた被保護データを変更することを妨げるシステムの実施例のブロックダイヤグラムである。

第９図は被保護領域内で所定のメモリロケーションにストアされた被保護データの変更を防ぐシステムの別の実施例のブロックダイヤグラムを示す。

第１０図は被保護領域がテストのためにアクセスされた時に制限を加えるチップ内被保護領域でのシステムの適当な実施例のブロックダイヤグラムである。

１０…チップ、１１…被保護領域、１４…マイクロプロセッサー、M_1，M_2，M_n…メモリ、１６…被保護データバス、１７…被保護アドレスバス、１８…移転ロジック回路、２０…パワー制御回路、ＳＣ…半導体基板層、DE_1…第１絶縁層、CN_1…第１導電層、DE_2…第２絶縁層、CN_2…第２導電層、Ｓ，Ｄ…拡散部分。

出願人代理人　弁理士　鈴江武彦

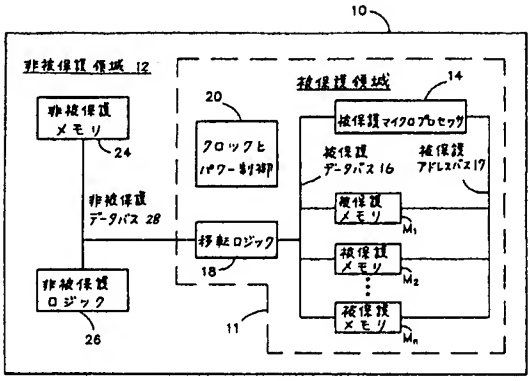


FIG. 1

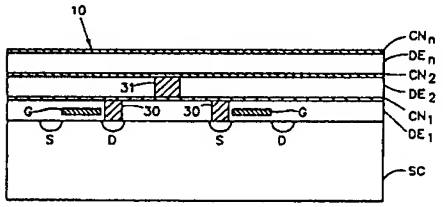


FIG. 2

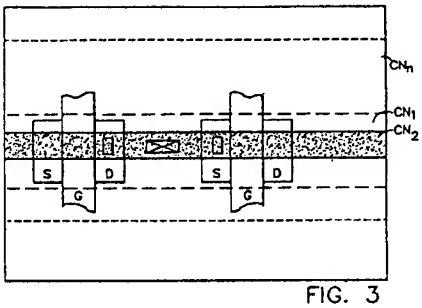


FIG. 3

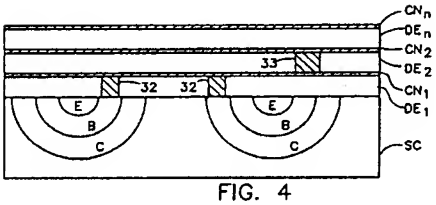


FIG. 4

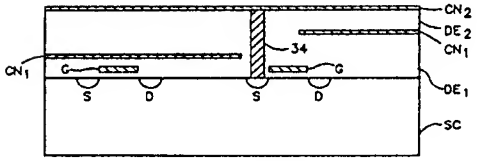


FIG. 5

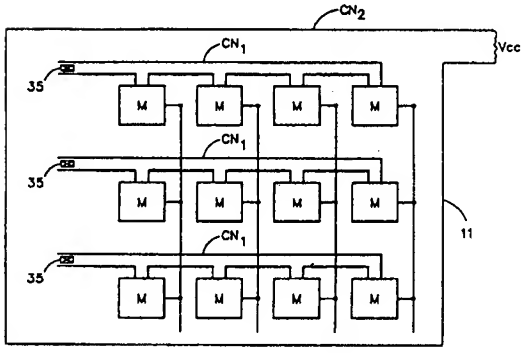


FIG. 6

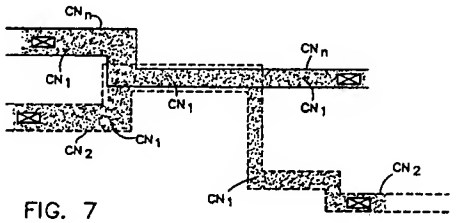


FIG. 7

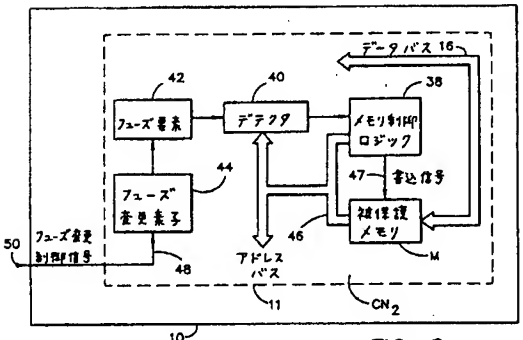


FIG. 8

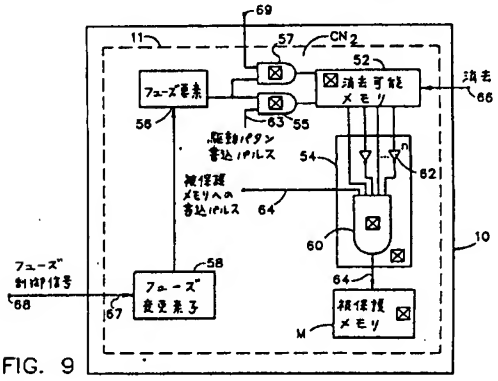


FIG. 9

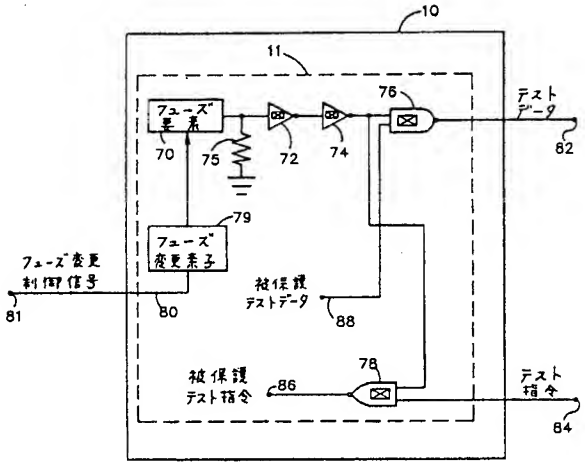


FIG. 10

第1頁の続き

⑤Int. Cl.[5]	識別記号	庁内整理番号
H 01 L 21/82 29/788 29/792		

⑦発 明 者 ボール・マロニー アメリカ合衆国、カリフオルニア州 92007、カーデイフ
ー バイー ザー シー、アボセツト・コート 1249

⑦発 明 者 ウイリアム・アレン・シユメイト アメリカ合衆国、カリフオルニア州 92116、サンデイエゴ、ビオナ・プレイス 4202